The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
08/11/2020

SUBJECT:
Multiple Vulnerabilities in Adobe Acrobat and Adobe Reader Could Allow for Arbitrary Code Execution (APSB20-48)

OVERVIEW:
Multiple vulnerabilities have been discovered in Adobe Acrobat and Adobe Reader, the most severe of which could allow for arbitrary code execution. Adobe Acrobat is a family of software developed by Adobe Inc. to view, create, manipulate, print, and manage files in PDF format. Adobe Reader is the free version within the Adobe Acrobat family of software. Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
There are no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Acrobat DC prior to version 2020.012.20041
- Acrobat Reader DC prior to version 2020.012.20041
- Acrobat 2020 prior to version 2020.001.30005
- Acrobat Reader prior to version 2020 2020.001.30005
- Acrobat 2017 prior to version 2017.011.30175
- Acrobat Reader prior to version 2017 2017.011.30175
- Acrobat 2015 prior to version 2015.006.30527
- Acrobat Reader 2015 prior to version 2015.006.30527

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**

- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Adobe Acrobat and Adobe Reader, the most severe of which could allow for arbitrary code execution. Details of the vulnerabilities are as follows:

- One disclosure of sensitive data vulnerability that could cause memory to be leaked. (CVE-2020-9697)
- One security bypass vulnerability that could allow an attacker to escalate privileges on an already compromised system (CVE-2020-9714)
- Two out-of-bounds write vulnerabilities that could lead to arbitrary code execution. (CVE-2020-9693, CVE-2020-9694)
- Two security bypass vulnerabilities that could lead to bypassing application security features. (CVE-2020-9696, CVE-2020-9703)
- Two stack exhaustion vulnerabilities that could cause application denial-of-service. (CVE-2020-9702, CVE-2020-9703)
- Eleven out-of-bounds read vulnerabilities that could cause information disclosure. (CVE-2020-9723, CVE-2020-9705, CVE-2020-9706, CVE-2020-9707, CVE-2020-9710, CVE-2020-9716, CVE-2020-9717, CVE-2020-9718, CVE-2020-9719, CVE-2020-9720, CVE-2020-9721)
- Five buffer error vulnerabilities that could lead to arbitrary code execution. (CVE-2020-9698, CVE-2020-9699, CVE-2020-9700, CVE-2020-9701, CVE-2020-9704)
- One user-after-free vulnerability that could lead to arbitrary code execution. (CVE-2020-9715, CVE-2020-9722)

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:
The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services

REFERENCES:
Adobe:
https://helpx.adobe.com/security/products/acrobat/apsb20-48.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9697

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9714
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9693
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9694
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9696
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9712
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9702
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9703
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9723
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9705
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9706
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9707
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9710
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9716
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9717
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9718
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9719
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9720
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9721
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9698
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9699
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9700
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9701
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9704
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9715
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9722